DETAILED ACTION

1. This office action is in response to a petition decision filed on 07/06/2010.

2. Claims 1-9 and 11 are pending.

3. Claim 1, 5, 6, 8, 9, and 11 are amended.

4. Claim 10 is canceled.

5. New 112 first paragraph rejection to claims 1, 5, 6, 8, 9 and 11 (see below).

6. Applicant's arguments with respect to claims 1-9 and 11 have been considered but are not persuasive.

Continued Examination Under 37 CFR 1.114

7. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/17/2009 has been entered.

Response to Arguments

8. Applicant, on pages 10-11, of the remarks, argues “Malcom does not teach an encryption rule storing portion that stores rule information that indicates an encryption rule for each secret level; a monitoring portion that monitors by confirming whether the information management system encrypted the information in accordance with the encryption rule based upon the process information received over the network from the information management system, and an information storing portion that stores the encrypted information; and [[a]]an encryption process confirmation portion that confirms whether the encryption of the information was performed in accordance with the encryption rule by transmitting, over the network to the encryption support system, process information indicating the encryption process performed by the encrypting portion and receives a confirmation result from the encryption support system.

Examiner respectfully disagrees and asserts that Malcom discloses that the operation of the system is controlled by policy data, which stores the corporation's regulations regarding security, authorization, and the actions that user's are permitted to perform, as well as operating information [para. 69; stores the…regulation regarding security equates stores rule information…an encryption rule…]. Malcom further teaches ensuring that the transmission data is transmitted at encryption strength appropriate to the contents of the transmission data; determining whether a check needs to be made as to whether a digital certificate received in transmission is valid [abstract; ensuring that the transmission data is transmitted at encryption strength corresponding to

monitoring portion that monitors by confirming whether the information management system encrypted the information…].

9. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claims as follows:

Claim Rejections - 35 USC § 112

10. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

11. Claims 1, 5, 6, 8, 9 and 11 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. In the above claims, the limitation: "by confirming" and "confirmation portion" in claim 5 are not described in the specification.

Examiner has considered the whole limitation: "a monitoring that monitors whether the information management system encrypted the information in accordance with the encryption rule based …" for examination purpose.

Claim Rejections - 35 USC § 102 or 103

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 1, 3, 5-9 and 11 are rejected under 35 U.S.C. 102(e) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Malcolm et al., Pub. No.: US 2004/0078334 A1.

Referring to claims 1, 5-6, 8 and 11, Malcolm teaches a security system comprising an information management system that manages information and an encryption support system that supports encryption of the information and in network communication with the information management system [abstract],

the encryption support system including:

an encryption rule storing portion that stores rule information that indicates an encryption rule for each secret level **[paras. 69 and 72;** regulations regarding security corresponding to encryption rule].

an encryption data transmitting portion that transmits encryption data that is necessary for encrypting information in accordance with the encryption rule over the network to the information management system **[paras. 248, 275 and fig. 17;** the sender's encryption key is transmitted with the message corresponding to transmits encryption data].

a process information receiving portion that receives process information which indicates an encryption process performed by the information management system, over the network from the information management system **[paras. 286 and 314]**.

a monitoring portion that monitors by confirming whether the information management system encrypted the information in accordance with the encryption rule based upon the process information received over the network from the information management system, and **[abstract, para. 278 and fig. 20 (see step S356);** the e-mail message is checked/monitored for encryption (encryption performed in accordance with policy data/encryption strength)].

a warning portion that warns the information management system over the network, if the monitoring portion has determined that the information is not encrypted in accordance with the encryption rule **[paras. 256, 269 and 297 and fig. 22]**, and

the information management system

including:

an encryption data receiving portion that receives the encryption data over the network from the encryption support system **[paras. 248, 275 and fig. 17],**

a classification secret level storing portion that stores classification of the information in connection with a secret level for each classification **[paras. 69, 72 and fig. 17]**,

an encrypting portion that specifies the classification of the information of the information and encrypts the information by using the received encryption data of the secret level for the specified classification **[paras. 286 and 314]**,

an information storing portion that stores the encrypted information **[paras. 69, 72 and fig. 17]**, and

a process information transmitting portion that transmits the process information over the network to the encryption support system **[paras. 248, 275 and fig. 17]**.

Referring to claim 3, Malcolm further teaches, wherein the information management system includes:

a classification secret level transmitting portion that transmits classification secret level information which indicates the classification and the secret level for the classification, over the network to the encryption support system **[paras. 248 and fig. 17]**, and

the monitoring portion of the encryption support system monitors whether the information is encrypted in accordance with the encryption rule by the information

management system based upon the process information received over the network from the information management system by comparing the received process information with the received classification secret level information **[abstract, para. 278 and fig. 20 (see step S356)].**

Referring to claim 7, Malcolm teaches a security system, further comprising a validity monitoring portion that monitors validity of an encryption rule that is used currently in accordance with vulnerability information about vulnerability of security received from a security information providing portion **[abstract, para. 278 and fig. 20 (see step S356)]**, wherein

the transmitting portion transmits the encryption data for changing the encryption rule appropriately to the information management system over the network, if decided that the encryption rule used currently has low validity **[paras. 248, 254-256, and 266]**.

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Malcolm et al., Pub. No.: US 2004/0078334 A1 in view of Iitsuka et al. US Patent No. 6,463,151.

Referring to claim 2, Malcolm teaches a security system comprising an information management system for managing information. Malcolm further teaches an encryption support system for supporting encryption of information in the information management system [see claim 1 above]. Malcolm does not explicitly teach a security system, wherein the rule information indicates the rule including an encryption system that is used for encryption and a valid term of an encryption key that is used for the encryption. However, Iitsuka teaches a security system, wherein the rule information indicates, as the encryption rule, a rule about cryptography and a valid term of an encryption key for encrypting the information,

if a period from the encryption process of the information to the present time exceeds the valid term for the encryption rule of the secret level for the classification of the information **[col. 3, lines 56-62 and fig. 4,** update the type of encryption by time scale according to a change over information/data i.e., copy one generation, copy freely and copy-prohibited (column 4, lines 45-50)],

the warning portion warns the information management system **[col. 9, lines 18-35; col. 12, line 63-col. 13, line 8 and figs. 2 and 4;** in-transition mode (01 is assigned in fig. 4) is equivalent to the warning portion warns/notifying the timing for changing over the key or encryption which inherently teaches a period or time should not be exceeds the valid term relevant to the rule of the secret level],

if the cryptography of the encryption rule is changed, the encryption data transmitting portion transmits the encryption data for performing encryption in accordance with the changed cryptography to the information management system **[col. 4, lines 33-39;** after update the type of encryption by time scale according to a change over information/data, transmission of encryption data will take place],

the warning portion warns the information management system to encrypt the information in accordance with the changed cryptography **[col. 9, lines 18-35; col. 12, line 63-col. 13, line 8 and figs. 2 and 4;** in-transition mode (01 is assigned in fig. 4) is equivalent to the warning portion warns/notifying the timing for changing over the key or encryption which inherently teaches a period or time should not be exceeds the valid term relevant to the rule of the secret level].

Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to modify the method of Malcolm to incorporate a valid term of an encryption key that is used for the encryption of Iitsuka because determining a key which is used for the encryption applied to transmitted data is changed depending on the content of copy management information for the data. Thus, the transmitted data can be further securely protected.

17. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Malcolm et al., Pub. No.: US 2004/0078334 A1 in view of Albrecht et al US Patent No. 6,510,521.

Referring to claim 4, Malcolm teaches a security system comprising an information management system that manages information. Malcolm further teaches an encryption support system that supports encryption of information in the information management system [see claim 1 above]. Malcolm does not explicitly teach the security system comprising a valid term managing portion that manages a valid term of a certification for affixing an electronic signature to the information. However, Albrecht teaches a security system comprising a valid term managing portion that manages a valid term of a certification for affixing an electronic signature to the information, wherein

the monitoring portion monitors whether or not it is necessary to affix a different electronic signature to the information in accordance with the valid term of the certification, and **[col. 1, lines 35-41;** "generates electronic signature and attached to a transferable unit of data" inherently teaches monitoring the information by affixing a different electronic signature to the information in accordance with the valid term of the certification].

the warning portion warns the information management system affix the different electronic signature to the information if it is decided that it is necessary to affix the different electronic signature **[col. 2, lines 57-62;** the electronic signature is attached at the time write data (system basic input/output service (BIOS) update, such as additions, deletions and modifications) is created, inherently teaches affix the different electronic signature to information].

Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to modify the method of Malcolm to incorporate a valid term of a certification for affixing a different electronic signature to information of Albrecht because generating and attaching electronic signature to a transferable unit prevents unauthorized write access to a protected storage such as FLASH memory.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YONAS BAYOU whose telephone number is (571)272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Yonas Bayou/
Examiner, Art Unit 2434
09/10/2009